Strategy Research Project

Open Source Cybersecurity for the 21st Century

by

Commander Gregory G. Allgaier
United States Navy

United States Army War College
Class of 2013

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
xx-03-2013	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Open Source Cybersecurity for the 21st Century

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Commander Gregory G. Allgaier
United States Navy

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Charles E. Grindle
Department of Distance Education

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5430

14. ABSTRACT

Due to the unique nature and global interdependence of cyberspace, traditional methods of security and deterrence are inadequate to defend against cyber threats. Cybersecurity in the 21st Century requires a new and open approach that incorporates assets from across the globe. Partnerships among cyberspace stakeholders, public, private, multi-national and non-governmental, require a secure global network for everyone. This paper argues the open and unregulated principles making the internet powerful also make it impractical to secure. Additionally, strategic response options are inadequate due to the level of anonymity provided to an attacker. A modern, partnership-based approach is the most appropriate way to secure the internet, much the same way as a neighborhood watch secures our residential community. Participation is voluntary and facilitated through an international organization, such as the UN. Finally, examples of open source cyber defense and free information exchange demonstrate the partnership-based methodology will work.

15. SUBJECT TERMS
Cyber Defense, Cyber Attack, Cyberpower, Internet, Information Assurance

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(Include area code)*
UU	UU	UU	UU	32	

USAWC STRATEGY RESEARCH PROJECT

Open Source Cybersecurity for the 21st Century

by

Commander Gregory G. Allgaier
United States Navy

Colonel Charles E. Grindle
Department of Distance Education
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title: Open Source Cybersecurity for the 21st Century

Report Date: March 2013

Page Count: 32

Word Count: 5430

Key Terms: Cyber Defense, Cyber Attack, Cyberpower, Internet, Information Assurance

Classification: Unclassified

Due to the unique nature and global interdependence of cyberspace, traditional methods of security and deterrence are inadequate to defend against cyber threats. Cybersecurity in the 21st Century requires a new and open approach that incorporates assets from across the globe. Partnerships among cyberspace stakeholders, public, private, multi-national and non-governmental, require a secure global network for everyone. This paper argues the open and unregulated principles making the internet powerful also make it impractical to secure. Additionally, strategic response options are inadequate due to the level of anonymity provided to an attacker. A modern, partnership-based approach is the most appropriate way to secure the internet, much the same way as a neighborhood watch secures our residential community. Participation is voluntary and facilitated through an international organization, such as the UN. Finally, examples of open source cyber defense and free information exchange demonstrate the partnership-based methodology will work.

Open Source Cybersecurity for the 21st Century

One of the primary functions of any government is to provide for the security of its citizens. The 2010 US National Security Strategy recognizes this by listing "the security of the United States, its citizens, and U.S. allies and partners" as one of America's enduring interests[1]. The other enduring interests are:

> A strong, innovative, and growing U.S. economy in an open international economic system that promotes opportunity and prosperity, respect for universal values at home and around the world, and an international order advanced by U.S. leadership that promotes peace, security, and opportunity through stronger cooperation to meet global challenges.[2]

In 2011, there were 11.6 million Americans reported to be victims of identity fraud,[3] which is a direct challenge to the security of U.S. citizens and hinders a strong and growing economy. According to President Obama, cybersecurity is one of the "most serious economic and national security challenges we face as a nation."[4] Secretary Napolitano has stated cybersecurity is an issue that influences everyone "from the kitchen table to the classroom, from business transactions to essential government operations and services."[5] Considering most households have home computers and there are enough mobile devices in the world for every living being to have one, cybersecurity is truly a global issue.

Due to the unique nature and global interdependence of cyberspace, traditional methods of security and deterrence are inadequate to defend against cyber threats. Cybersecurity in the 21st Century requires a new and open approach that incorporates assets from across the globe. Partnerships among cyberspace stakeholders, public, private, multi-national and non-governmental, will be required to secure the global network for everyone. Open and unregulated principles make the internet powerful, but

also make it impractical to secure and strategic response options are inadequate due to the level of anonymity provided to an attacker. A modern, partnership based approach is the most appropriate way to secure the internet, much the same way as a neighborhood watch secures our homes. The Department of Homeland Security should be responsible for implementation, with the Department of Justice charged with domestic enforcement and the Department of Defense responsible for external response/cyber attack.

There are many examples of cyber attacks against the United States. In 2008, the Department of Defense suffered a major compromise of its networks by a malicious code placed on a USB thumb drive.[6] The code infected a U.S. military computer, then uploaded itself and spread across the classified and unclassified networks. Former Deputy Defense Secretary William J. Lynn III called this event "the most significant breach of U.S. military computers ever"[7] and served as a catalyst to change DOD network security practices and procedures. Unfortunately, cyber attacks do not exclusively target military networks. In September 2012, six major American banks suffered from a denial of service attack preventing customers from accessing their accounts or paying their bills.[8] In both cases, the attack originated from outside of the border of the United States and demonstrated the global reach of the cyber domain. These two examples show the need for comprehensive security strategy to protect the economic and national security infrastructure of the United States.

Cybersecurity is an incredibly complex issue. First, the cyber domain spans the globe. Malicious actions are no longer constrained by national borders and it can be tough for the targeted nation to respond without violating the sovereignty of the nation

where the attack originated. Secondly, cyberspace is relatively anonymous; there are many methods, some much more sophisticated than others, for a determined aggressor to conceal his/her identity. Third, the cost of entry into the cyber domain is relatively cheap. Cybersecurity issues are further complicated through a lack of common understanding. A framework for cyber defense does not yet exist, what constitutes a cyber attack has not been defined, nor have strategic applications of cyberpower been developed. While cyberpower's contribution to national security is not fully developed, potential avenues of strategy include use as an intelligence tool, as the mechanism for an assault, as a method to strengthen traditional hard power components, as a means to undermine an adversary's hard power, and as a tool to bolster or break moral. [9]

Critical U.S. industries, such as the telecommunications, energy, and finance depend on cybersecurity in order to operate safely. Minor interruptions can easily create negative effects ranging from the nuisance of the loss of a local ATM to a citywide shutdown of the electric grid. Secretary Panetta has warned a collective attack against critical infrastructures, especially combined with a physical attack on the U.S. has the potential to become a "cyber Pearl Harbor".[10] As a result, cyber defense has risen to the forefront of security issues. However, due to the revolutionary nature of cyber warfare, and to a lesser extent, 21st century warfare itself, a new approach is required. The traditional methods of security and deterrence will not be as effective as they were in previous centuries. Modern cyber defense requires a new and open approach which incorporates assets from across the globe. Partnerships amongst cyberspace stakeholders, public, private, multi-national and non-governmental, will be required to secure the global network for everyone.

Two key attributes making the cyber domain unique is it is universally accessible and extremely fast. Societies have competed for land and maritime security for centuries, but traveling any meaningful distance takes days. 20th century technology created the air and space domains, but even after over 100 years of aviation, specialized equipment and training are required to overcome the natural limits of gravity. While it may take sophisticated equipment and specific skills to dominate cyberspace, the design of the World Wide Web permits access by anyone from almost anywhere in the world.

"The internet was based on the idea there would be multiple independent networks of rather arbitrary design".[11] Robert Kahn initially conceived the open-architecture which would eventually develop into Transmission Control Protocol/Internet Protocol (TCP/IP) based on the following ground rules:[12]

- Each distinct network would have to stand on its own and no internal changes could be required to any such network to connect it to the Internet.
- Communications would be on a best effort basis. If a packet did not make it to the final destination, the source would retransmit it shortly.
- The networks would be connected using black boxes called gateways and routers. The gateways would not retain information about the individual flow of packets passing through them, thereby keeping them simple and avoiding complicated adaptation and recovery from various failure modes.
- There would be no global control at the operations level.

Because of open architecture, the modern day internet is a sprawling web of interconnected networks keeping digital information flowing. Individual computers

connect to Internet Service Providers (ISPs) through dedicated data lines, cable or phone modems, or satellite antennas. The ISPs, in turn, connect through several high-level networks through various Network Access Points (NAPs). Since the internet developed with an open architecture, there is no overall controlling network. Switches and routers automatically control the flow of information from origin to destination. Open architecture principles worked well for the early development and explosive growth of the internet, but also created the underlying challenge of securing it. Three ways open architecture contributes to the challenge of cybersecurity are a relatively high level of anonymity, limited regulation, and no universal structure.

Through the nature of its design, open architecture results in high level of anonymity. The internet's design permits any device conforming to modern day protocol standards (TCP/IP being the most prevalent) to communicate across the network without needing to authenticate its identity, so there are steps a user can take to protect their identity, IP address, and network activity. Furthermore, political and social organizations deem anonymous communications essential to open and honest discussions. The U.S. Constitution protects anonymous communications under the First Amendment. The 1995 Supreme Court ruling in McEntyre v. Ohio states

> Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical minority views…Anonymity is a shield from the tyranny of the majority…It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation…at the hand of an intolerant society.[13]

Hiding the identity of users and systems makes cybersecurity a challenge because the originator or point of origin of malicious messages or code is hard to determine. Without a known source, cyber defense efforts cannot focus on a particular or likely threat. In

addition, the anonymity inherent in cyberspace increases the difficulty of finding and prosecuting the attacker.

The open architecture principles of each network standing on its own and no global control led to limited regulation of the internet. These principles encouraged rapid development of the internet primarily because anyone could contribute to its development and the best mechanisms succeeded on their merit. The World Wide Web flourished, but consequently created an environment without a regulating authority to assist in cyberspace security. Without a regulating authority, compliance with security protocols and procedures is voluntarily and there are no universal mechanisms for restricting or even refusing access for violations or criminal activity. Recent attempts to increase regulation of the internet have been unable to reach a consensus. For example, delegates from The United States, United Kingdom, Canada, and Australia walked away from the World Conference on International Telecommunications in December 2012, out of concern interpretations of proposed internet telecommunications regulations may give the UN control over elements of the internet and lead to increased powers of censorship.[14] While increasing regulation of the internet would make security easier, it comes with a risk of perceived censorship nations are unlikely to accept.

In addition to limited regulation and anonymity, open architecture fostered an internet without the need for a universal structure. Developers were free to create the hardware and software to make their individual networks. As long as the networks followed internet protocols, they could interconnect. Gateways and routers autonomously manage communications between networks and look for the most efficient pathway to send information packets from origin to destination, regardless of

the manufacturing specification of the device. As a result, modern computers and mobile devices can exchange information regardless of operating system, internet service provider, or cellular carrier. The challenge of securing cyberspace with a variety of devices increases because each device has unique vulnerabilities. Security solutions require versions developed for each unique operating system, hardware build, or software configuration. Each of the multiple pathways interconnecting the internet represents a potential avenue for exploitation.

Anonymity, limited regulation, and lack of universal structure were essential to the explosive growth of the internet, but created an easily exploitable environment. These factors, coupled with the internet's global reach and low cost of entry, are what make securing the cyber domain one of the most complex challenges we face as a nation. Secretary Panetta called cyberspace "the new frontier, full of possibilities…but full of new perils and new dangers"[15] as part of his speech explaining the DoD's increased role in cyber defense. While the Defense Department is responsible for national defense, the unique nature of preventing cyber attack requires a coordinated effort across all the departments of the U.S. government.

While all departments of the U.S. government share responsibility for national security, the Departments of Defense and Homeland Security share the lead in defending the homeland against cyber attack. DHS is responsible for domestic cybersecurity through its National Cyber Security Division (NCSD) which "works collaboratively with public, private and international entities to secure cyberspace and America's cyber assets."[16] The NCSD achieves its strategic objectives through the

National Cyberspace Response System, the Federal Network Security branch, and Cyber-Risk Management Programs.

DoD has traditionally been responsible for defending its internal networks, but recently claimed an increased role in protecting cyberspace during a speech presented by Secretary Panetta. While reiterating the Department of Defense's "supporting role" in cyber defense, he laid out three areas of focus: developing new capabilities, putting in place the policies and organizations needed to execute the mission, and building effective cooperation with industry and international partners.[17]

The Departments of State and Justice also play an important role in securing cyberspace. Because the cyber domain crosses international borders, the State Department has a role in building international consensus regarding the roles and responsibilities of nations in securing cyberspace. The Justice Department, namely the FBI, assists in cybersecurity by investigating and prosecuting cyber attacks as well as preventing cyber crime within the U.S.

Traditionally, the United States has protected its borders and citizens through strong defensive measures. Individuals and cargo enter the U.S. through checkpoints where Customs and Border Protection prevent illegal entry while facilitating lawful international trade and travel.[18] Immigration and Customs Enforcement enforces federal laws governing border control, customs, trade, and immigration.[19] The FBI and other law enforcement agencies at the state and local level serve and protect U.S. citizens and enforce the laws within their jurisdictions. The U.S. military counters external threats through offensive and defensive operations within the land, air, and maritime domains.

While each organization makes unique contributions to national security, they rely on two commonalities: they can identify the source of the threat and they can restrict the approach of the threat. When defending against cyber threats, it is not always possible to identify the source of the threat. The anonymity inherent in cyberspace permits an attacker to conceal their identity. Due to the controversial nature of censorship, a requirement for a user to reveal their identity is unlikely. Furthermore, since individuals, non-government organizations, and third world governments can afford the cost of entry into cyberspace, cyber defense planners cannot reduce the list of potential threats to a manageable level based on capabilities or resources. Traditional security measures often include borders to redirect avenues of approach toward established access points where agents and other entities can monitor and restrict entry as required. When defending against cyber threats, the approaches are global. The autonomous routing of packets of information permits instantaneous redirection throughout the World Wide Web. Information in cyberspace travels at the speed of light, so the redirections can send packets around the world multiple times with minimal interruption or impact. The unique challenges associated with identifying the source and restricting the approach of a cyber attack make traditional security methods inadequate for modern day cyber defense.

There is another key reason traditional security measures are inadequate for cyber defense. Users depend on it for daily operations. Unlike traditional security measures restricting access or entry, global reliance on the internet prevents simply turning it off or pulling the plug to prevent an attack. Users have unique requirements and come from diverse backgrounds, domestic and international as well as the public

and private sectors. They rely on the internet for just about every daily task, ranging from personal finance to controlling the electrical grid, from private communications to public announcements. In other words, it is too big to control and too important to turn off.

A relatively modern method for achieving national security, especially at the strategic level, is through deterrence. As a strategy, deterrence gained prominence during the Cold War to prevent total war between the U.S. and USSR by promising unacceptable consequences for a nuclear attack. In November 2011, the Department of Defense Cyberspace Policy Report states "deterrence in cyberspace, as with other domains, relies on two principal mechanisms: denying an adversary's objectives and, if necessary, imposing costs on an adversary for aggression."[20] In a 2009 RAND report, Martin Libicki offers three critical differences between cyber deterrence and general military (or nuclear) deterrence. Posed in the form of questions, they are: "Do we know who did it? Can we hold their assets at risk? Can we do so repeatedly?"[21] Effective deterrence requires three things. First, the deterring state needs to know who attacked it, and it must convince itself, as well as third parties, they have correctly attributed responsibility for the attack.[22] Second, the deterring state needs to know what targets are vulnerable, their degree of vulnerability, and their recoverability. Without this knowledge, it is difficult to know (and promise) the extent of the retaliatory damage.[23] Third, by initiating a retaliatory response, the deterring state exposes the attacker's vulnerability and system administrators have the opportunity to fix it.[24] These critical differences demonstrate key deficiencies of deterrence in the cyber domain.

Deterrence could also be asymmetric by threatening a traditional military response for a cyber attack. Determining a target's vulnerability and recoverability becomes the same calculation applied to deterring traditional threats, and the deterring state has the option of repeating the retaliation as often as necessary to prevent further attacks. However, the need to identify the source of the attack remains unresolved. Without attribution, imposing costs for aggression will not deter a cyber attack. Since attribution is not required to deny an adversary's objectives, deterrence can contribute to defending the internet, but even with traditional security methods, it is not enough. A new, open approach to cyber defense is required.

"Open source security is about connecting the international, the interagency, the private-public and lashing it together with strategic communications."[25] It is no surprise cyberspace's global interdependency and speed of light information exchange requires vigilance by all of its users. An open source approach ties that vigilance together through the sharing of information regarding ongoing or pending attacks. The Atlantic Council has reported achieving cyber stability requires "…a three-legged stool of resilience, cooperation, and transparency."[26] These three legs of their stool help to describe open source approach to cybersecurity.

Achieving resilience in cyberspace requires efforts at the user, ISP, and national levels. Users have a responsibility to ensure they protect their computers through anti-virus and firewalls. These are readily available commercially, with companies such as Norton, McAfee, and Kaspersky offering a variety of products ready to meet the consumer's individual needs. Considering every computer connected to the internet represents a potential security vulnerability, an open source approach should include a

strategic communication message to individual users explaining the importance of having effective anti-virus and firewall protection on their computers.

ISPs also have a responsibility to achieving resilience in cyberspace. Unlike individual users, ISPs provide a portion of the network and have trained professionals charged with monitoring their network. ISPs contribute to achieving resilience by ensuring sufficient redundancy in their network architecture in order to reroute communication should a portion of the network come under attack. Furthermore, through vigilant monitoring, cyber attacks can be promptly recognized and defeated before they can cause an appreciable level of damage.

The U.S. Government also has a responsibility to provide resiliency in cyberspace. Networks interconnect through cables and access points that have physical locations. Each of these represents potential targets requiring physical protection by civil authorities at the local, state and federal levels. In addition, Federal Agencies such as the National Security Agency (NSA), the FBI, and the DoD have a responsibility to share technical expertise and national Intelligence in order to assist ISPs and other cyberspace stakeholders in defending their networks. Because the internet has global dependency and reach, the U.S. Government contributes to building international partnerships by sharing the same types of expertise and intelligence it shares with the private sector. Public, private, and international cooperation are critical elements for any open source security solution.

Cooperation is the second leg of the cyber stability stool and is arguably the most important for open source cybersecurity. Since the internet travels through the global commons, independent states have a shared responsibility for cyber defense, especially

when considering the hardware that makes up the internet resides within sovereign territory. The U.S. strategy for cyberspace advocates this international cooperation and will "… work to create incentives for, and build consensus around, an international environment in which states…work together and act as responsible stakeholders."[27] In addition to working with the international community, cooperating with the private sector is an essential element for securing cyberspace.

Critical industries, such as telecommunications, energy, and finance, have become dependent on feely operating in cyberspace. They are also among the most common targets for cyber attack. In February 2013, an intelligence estimate named energy, finance, information technology, aerospace and automotives as examples of the wide range of sectors targeted by foreign hackers.[28] By exchanging information, private industries and the government can establish a coordinated response to cyber attacks. In addition, since private industry develops the majority of the devices connected to the internet, their corporate knowledge of system functionality is invaluable to developing robust cyber defenses and managing an appropriate response to cyber attacks. Finally, by simply sharing information about cyber threats predicted by the intelligence community or observed by private users strengthens cooperation between the public and private sectors and builds trust through transparency.

Transparency is the third leg of the cyber stability stool and is the foundation for meaningful open source cybersecurity. Developing an open approach involving public government, the private sector and the international community requires relationships built on trust. Furthermore, a weakness in any sector of the internet, regardless if it is public, private, or international, represents a potential vulnerability to exploit and used to

target another sector. U.S. cyber strategy states “no one nation can have full insight into the world’s networks; we have an obligation to share our insights about our own networks and collaborate with others when events might threaten us all.”[29] Sharing pertinent information between the private and public sectors, as well as with foreign partners and international organizations is one key way to build the relationships necessary for open security.

Transparency helps to codify acceptable behavior on the internet. The international community does not always share the same values, so activity considered a cyber attack in one state may be acceptable behavior in another. Likewise, security restrictions may be acceptable to some cultures, but considered censorship to others. Understanding these diverse perspectives is crucial to developing meaningful open source cybersecurity, but requires national or organizational transparency regarding their policies, beliefs, and values.

There are three advantages for open source cybersecurity: it is mutually acceptable to all stakeholders, it is practical, and solutions come from diverse perspectives. First, open source cybersecurity is mutually acceptable to all stakeholders primarily because it is a collaborative effort. Recent attempts in the U.S. to legislate cybersecurity failed because business groups felt it would burden them with mandatory security measures and civil liberty groups believed it would permit spying on internet users.[30] International attempts to increase the regulation of telecommunications through the UN have also recently failed due to fears of increased censorship.[31] These examples demonstrate the futility of reaching global consensus on internet regulation. By relying on voluntary partnerships vice mandatory regulation, open source

cybersecurity rises above the concerns of mandatory restrictions and facilitates acceptance through organizational buy-in.

A second advantage to open source cybersecurity is its practicality. By its nature, regulation requires the standardization of cyber incident reporting procedures, security software, operating systems, and business practices. Open architecture was used to develop the internet, so standardization would require extensive changes to existing (and fully functioning) infrastructure. In contrast, implementing an open source solution does not require standardizing the internet, thus saving money, time, and resources.

A third advantage to open source cybersecurity is solutions come from diverse perspectives. By including public, private, multi-national and non-governmental stakeholders, new attitudes, global and cultural understanding, and greater insight will create innovative approaches to tackle the complexity of cybersecurity. In turn, a diverse approach to cybersecurity will reinforce the previously mentioned advantage of mutual acceptance.

There are several disadvantages to open source cybersecurity. First, there is no controlling organization or agency. Since sharing information between stakeholders is voluntary, there is no guarantee partners will offer the necessary details regarding a pending attack or potential vulnerability. Similarly, the decision to respond to an announced threat or vulnerability rests with each stakeholder. While they may share how they choose to respond, cooperative cyber defense ultimately relies on the stakeholder to take the appropriate action.

A second disadvantage to open source security is it relies on freely exchanging information. Several civil liberty groups view freely exchanging information as a release of private details to the public or the government and would loudly protest sharing information. In addition, the world does not universally accept the democratic value of free speech. As a result, information provided by some non-democratic nations may be doctrinally biased, or not even shared if it can be considered embarrassing.

A third disadvantage to open source cybersecurity is its effectiveness is difficult to measure. Successful cyber attacks are relatively easy to detect. In contrast, it is impossible to quantify the number of attacks not attempted or prevented due to increased vigilance and resilience. Furthermore, there is no way to know for certain if defensive measures in response to a potential cyber threat were the reason the threat did not materialize, or if the threat was never real.

There are several risks to implementing open source cybersecurity. First, sharing information between stakeholders runs the risk of spilling classified data or compromising collection methods. A second risk is shared information can be exploited. Tomorrow's cyber adversary could be today's cybersecurity partner. A third and most likely risk is attaining a sufficient level of collaboration required for meaningful open source cybersecurity. Developing standard procedures and elements of cooperation, such as the ones described below, mitigates these risks.

Expanding the principles contained in President Obama's executive order for improving critical infrastructure cybersecurity[32] into an international agreement is one way the U.S. could lead the international community to establishing an open source approach to cyber defense. For the agreement to be viable, it must increase the

volume, timeliness, and quality of information shared with participating nations and organizations, including classified information when warranted. For the agreement to be acceptable, it must protect the fundamental privacy and civil liberties each partner values. For the agreement to be amenable, it must include consultation and cooperation among all participants, regardless if they are public, private, foreign, or non-governmental. Finally, for the agreement to be meaningful, it must establish a framework of accepted methodologies and practices to standardize the procedures used by all participants.

Participation would be voluntary and ideally facilitated through an international organization. While several international forums are appropriate, the United Nations is exceptionally suitable due to its world-wide membership and history for addressing international security challenges. Partner nations would agree through a formal international agreement to honestly share information, enforce appropriate behavior, recognize sovereign values of privacy and civil liberty, and conform to established standards and procedures. A common reporting system would need to be established and an international operations center established responsible for centralized reporting, responding, and coordination as well as providing office spaces and conference facilities. As the sponsor, the U.S. should offer initial space, but as the program expands, other nations could host satellite centers. Cost sharing is negotiable, but should ensure no participant accepts an exceptionally disproportionate share of the financial burden.

Implementation will be challenging for many reasons. First, this paper has already discussed existing futile attempts to reach an international consensus regarding

cybersecurity. Barring a significant cyber related attack, there is no reason to anticipate a significant change in global opinion. Even if an internationally accepted forum, such as the United Nations, reached an agreement, it would have limited applicability to the private sector.

Franklin Kramer offers an approach the U.S. can take to promote participation. Recognizing "cybersecurity is inherently a complex environment and it becomes more complex the more entities are involved in decision making"[33], he proposes focusing on a small group of "like-minded entities"[34] to establish a cooperative effort. Starting with a small group of organizations with similar goals facilitates consensus because of the reduced potential for disagreement. Once a core of participants is established, they can develop acceptable behavioral norms and common standards to provide mutually supportive cybersecurity. By successfully mitigating cyber threats, the partnership increases its appeal, and additional groups (public, private, international, or non-governmental) are willing to accept the established terms of agreement and join the open source cybersecurity network.

There are several U.S. Government led initiatives for developing open source solutions to cybersecurity. One example is the NSA Award for the Best Cybersecurity Paper. The NSA established the award "to encourage the development of the scientific foundations of cybersecurity."[35] Nominated papers may come from any field of cybersecurity research and are not limited to U.S. Citizens. While the NSA Director of Research determines the winner, a distinguished panel of experts from various civilian institutions provides individual assessments regarding the "scientific merit and significance of the work reported [and] the degree to which the paper exemplifies how to

perform and report scientific research in cybersecurity."[36] By establishing an initiative combining civilian and government expertise to recognize and promote research in cybersecurity by the civilian, government, and international community, the NSA demonstrates one approach to open source security.

Another example of the U.S. Government developing open source solutions for cybersecurity is DHS awarding 34 contracts for cybersecurity research and development. DHS solicited proposals "aimed at improving security in federal networks and across the Internet while developing new and enhanced technologies for detecting, preventing and responding to cyber attacks on the nation's critical information infrastructure."[37] Awards went to 29 academic and research organizations outside of the U.S. Government and funding for four of the contracts were from international partners.[38] These research contracts demonstrate DHS's willingness to broaden their approach to cybersecurity by including the diverse perspectives from across the nation and contributing to the similar goals of our international partners.

In addition to U.S. Government led initiatives, there are also examples of open source solutions for cybersecurity offered by the private sector. One example is the Financial Services Information Sharing and Analysis Center (FS-ISAC). As the "the only industry forum for collaboration on critical security threats facing the financial services sector,"[39] the FS-ISAC quickly disseminates timely information between the public and private organizations regarding cybersecurity threats to the financial services sector. The FS-ISAC is a non-profit, privately owned organization with a representative Board of Directors elected by its members.[40] Its mission is to "collaborate with the U.S. Department of Treasury (Treasury) and the Financial Services Sector Coordinating

Council, to enhance the ability of the financial services sector to prepare for and respond to cyber and physical threats, vulnerabilities and incidents, and to serve as the primary communications channel for the sector."[41] While membership is not mandatory, Treasury, DHS, the Office of the Comptroller of Currency, the United States Secret Service, and the Financial Services Sector Coordinating Council all recommend it. Furthermore, it is the primary means for Treasury and DHS to promulgate critical information to the financial sector in a time of crisis. As a privately established organization to meet the need for public and private sectors to share information about cyber threats, the FS-ISAC exemplifies privately led open source solutions for cybersecurity. Furthermore, the principles behind the establishment of the FS-ISAC demonstrate the need for collaborative reporting. Applying elements of this private organization on a global scale provides another approach to international open source cybersecurity.

There are also international examples of open source cybersecurity. The International Cyber Security Protection Alliance (ICSPA) is one example of a privately owned organization in the United Kingdom "focused on helping provide resource support directly to law enforcement cyber crime units, thereby to help increase the capability and capacity of those agencies in countries which face the greatest cyber challenges."[42] Through its International Cybercrime Assistance Programme, the ICSPA provides resources to accepting countries to support their law enforcement efforts against cyber crime.[43] In addition, the ICSPA recognizes countries with advanced capabilities, such as the U.S., Australia, Canada, and South Africa, still have resource shortfalls, so they established the National Cybercrime Assistance Programme to

provide additional funding and other support.[44] By providing resources to willing countries, the ICSPA assists worldwide cyber defense and exemplifies open source cybersecurity.

Securing the internet is an extremely complex issue due the number of users, global reach, and international dependence. Critical industries, such as the telecommunications, energy, and finance depend on a secure and reliable internet to operate safely. Open source cybersecurity provides a modern, partnership-based approach to securing the internet. The same open and unregulated principles credited for the development of a powerful internet make open source cybersecurity viable. The opportunity to detect a pending cyber threat is improved by increasing the number of observers monitoring the internet and sharing information. Elements of cybersecurity, as well as larger national security, will always rely on traditional security and deterrence, but the increased vigilance provided by public, private, multi-national and non-governmental stakeholders is essential for securing cyberspace in the 21st century.

Endnotes

[1] Barack H. Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 7.

[2] Ibid.

[3] Javelin, *2012 Identity Fraud Industry Report: Social Media and Mobile Forming the New Fraud Frontier*, https://www.javelinstrategy.com/brochure/239 (accessed February 21, 2013).

[4] Barack H. Obama, *Remarks by the President on Securing Our Nation's Cyber Infrastructure* (Washington, DC: The White House, May 29, 2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (accessed February 21, 2013).

[5] Department of Homeland Security, *Secretary Napolitano Launches National Cyber Security Awareness Month 2012* (Washington, DC, U.S. Department of Homeland Security, October 1, 2012), http://www.dhs.gov/news/2012/10/01/secretary-napolitano-launches-national-cyber-security-awareness-month (accessed February 21, 2013).

[6] William J. Lynn, III, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (Sep/Oct 2010): 97-108, http://search.proquest.com.ezproxy.usawcpubs.org/docview/749414296/13C6594DC307D58D4BF/8?accountid=4444 (accessed February 21, 2013).

[7] Ibid., 97.

[8] Nicole Perlroth, "Attacks on 6 Banks Frustrate Customers," *New York Time*, September 30, 2012, http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html?_r=2&

[9] Danny Steed, "Cyber Power and Strategy - So What?" *Infinity Journal* 1 no.2 (Spring 2011): 21-24, https://www.infinityjournal.com/article/11/Cyber_Power_and_Strategy__So_What/ (accessed February 21, 2013).

[10] Leon E. Panetta, *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security*, (Washington, DC: U.S. Department of Defense, October 11, 2012), http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136 (accessed February 21, 2013).

[11] Barry M. Leiner, et al., "Brief History of the Internet," Internet Society, http://www.internetsociety.org/brief-history-internet (accessed February 21, 2013).

[12] Ibid.

[13] McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).

[14] David Meyer, "ITU Chief Claims Dubai Meeting 'Success', Despite Collapse of Talks," ZDNet, http://www.zdnet.com/itu-chief-claims-dubai-meeting-success-despite-collapse-of-talks-7000008808/ (accessed February 21, 2013).

[15] Panetta, *Remarks by Secretary Panetta on Cybersecurity*.

[16] Department of Homeland Security "National Cyber Security Division," http://www.dhs.gov/national-cyber-security-division (accessed February 23, 2013).

[17] Panetta, *Remarks by Secretary Panetta on Cybersecurity*.

[18] Department of Homeland Security, "About CBP," http://www.cbp.gov/xp/cgov/about/ (accessed 23 February 21, 2013).

[19] Department of Homeland Security, "About ICE," http://www.ice.gov/about/overview/ (accessed 23 February 21, 2013).

[20] U.S. Department of Defense, *Department of Defense Cyberspace Policy Report A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934 (November 2011)*. Open-file report, U.S. Department of Defense. Washington, DC, 2011, http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf (accessed February 23, 2013).

[21] Martin C. Libicki, *Cyber Deterrence and Cyberwar*, (Santa Monica, CA: RAND Corporation, 2009), 39.

[22] Ibid., 42.

[23] Ibid., 52-54.

[24] Ibid., 54-55.

[25] James Stavridis, "James Stavridis: A Navy Admiral's Thoughts on Global Security," (lecture, TEDGlobal 2012, Edinburgh, Scotland, June 26, 2012), http://www.ted.com/talks/james_stavridis_how_nato_s_supreme_commander_thinks_about_global_security.html (accessed February 23, 2013).

[26] Franklin D. Kramer, *Achieving International Cyber Stability* (Washington, DC: Atlantic Council, September 2012), 3.

[27] Barack H. Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011), 11.

[28] Ellen Nakashima, "U.S. Said to be Target of Massive Cyber-espionage Campaign," *Washington Post*, February 10, 2013, http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html (accessed 23 February, 2013).

[29] Obama, *International Strategy for* Cyberspace, 19.

[30] Andrew Couts, Senate Kills Cybersecurity Act of 2012," *Digital Trends*, August 2, 2012, http://www.digitaltrends.com/web/senate-votes-against-cybersecurity-act-of-2012/ (accessed 23 February, 2013).

[31] David Meyer, "ITU Chief Claims Dubai Meeting 'Success', Despite Collapse of Talks," ZDNet, http://www.zdnet.com/itu-chief-claims-dubai-meeting-success-despite-collapse-of-talks-7000008808/ (accessed February 21, 2013).

[32] Barack H. Obama, *Executive Order – Improving Critical Infrastructure Cybersecurity* (Washington, DC: The White House, February 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (accessed February 25, 2013).

[33] Kramer, *Achieving International Cyber Stability*, 11.

[34] Ibid.

[35] Cyber-Physical Systems Virtual Organization, "NAS Award for the Best Scientific Cybersecurity Paper," http://cps-vo.org/group/sos/papercompetition (accessed 24 February 2013).

[36] Ibid.

[37] Department of Homeland Security, *DHS Science and Technology Directorate awards 34 contracts* (Washington, DC, U.S. Department of Homeland Security, October 24, 2012), http://www.cyber.st.dhs.gov/wp-content/uploads/2012/11/Press-Relase_cyber-contracts-FINAL.pdf (accessed February 24, 2013).

[38] Ibid.

[39] Financial Services Information Sharing and Analysis Center, "Financial Services Information Sharing and Analysis Center," https://www.fsisac.com/ (accessed February 24, 2013).

[40] Financial Services Information Sharing and Analysis Center, " FS-ISAC Ownership," https://www.fsisac.com/about/ownership (accessed February 24, 2013).

[41] Financial Services Information Sharing and Analysis Center, "Mission," https://www.fsisac.com/about/mission (accessed February 24, 2013).

[42] International Cyber Security Protection Alliance, "What's Different About the ICSPA," https://www.icspa.org/about-us/whats-different-about-the-icspa/ (accessed February 24, 2013).

[43] International Cyber Security Protection Alliance, "The International Cybercrime Assistance Programme," https://www.icspa.org/activities/work-programmes/the-international-cybercrime-assistance-programme/ (accessed February 24, 2013).

[44] International Cyber Security Protection Alliance, "The National Cybercrime Assistance Programme," https://www.icspa.org/activities/work-programmes/the-national-cybercrime-assistance-programme/ (accessed February 24, 2013).